REMARKS

Reconsideration of the above referenced application in view of the enclosed amendments and remarks is requested. Claims 1, 8, and 21-23 are amended. Claims 1, 4, 6-8, 11, and 21-31 remain in the application.

The Applicants thank the Examiner for the telephonic interview held on December 27, 2006.

ARGUMENT

Claims 1, 4, 6-8, 11, and 21-31 are rejected under 35 USC 102(b) as being anticipated by Herz, et al. (6,088,722)(hereinafter Herz).

Claim 1, as amended, recites downloading an update for the cryptographic software resident on the client device from the server, the content protection software, when executing on the client device, for decrypting the PPV audio-visual content, controlling consumption of the PPV audio-visual content, and deterring unauthorized access to the content, the downloading being performed *when the received billing log data indicates past consumption of PPV audio-visual content by the client device at less than a predetermined threshold for the selected period of time.*

Claim 1 requires that cryptographic software for deterring unauthorized access to the content on the client device is updated based on certain conditions. *Herz teaches that an EPG is updated on the set top box based on user's viewing habits. More particularly, Herz teaches that EPG* ***data*** *is updated.* That is, the EPG data that describes which TV programs are to be broadcast at which times is updated, NOT the cryptographic software (e.g., digital rights management (DRM) software) on the set top box that decrypts the encrypted broadcast data (e.g., TV programs or PPV movies) and displays it in response to a viewer command. Herz does not teach or suggest updating cryptographic software on the client device at all. EPG data is very different than cryptographic software! Cryptographic software

is software that is used to decrypt encrypted content in a controlled manner in a client device (such as a set top box) so that the high value content cannot be pirated. EPA data is merely the data describing the current and upcoming broadcast schedule of broadcasters in a cable or satellite TV system. Updating EPG data does not disclose updating cryptographic software, since EPG data is not software and EPG data does not protect the content.

Herz does not teach or suggest at least one of the claimed limitations. Therefore, a valid case for anticipation has not been made and independent claim 1 is allowable as presented.

The Examiner seeks to rebut the above argument in the Office action dated November 30, 2006. However, the Office action does not address the specific argument made by the Applicant. The Applicant contends the Examiner is misreading the teachings of the Herz reference and a case for anticipation has not been made. The Examiner is wrong in his characterization of the teachings of Herz and is improperly reading the term "content protection software" to include EPG data. Herz teaches updating EPG data based generally on viewer profiles. Herz does not teach that the cryptographic software (e.g., the DRM application) on the set top box is updated when the viewer's actual PPV activity is too low. Nonetheless, the claims have been amended to more particularly recite the claimed invention. This rejection must now be withdrawn.

Claims 4, 6, and 7 depend from allowable independent claim 1. Hence, they are also allowable.

Claims 24-27 are also dependent on claim 1, so they are also allowable.

Furthermore, with respect to claim 24, it requires that the updated content protection software includes a new cryptographic technique. A cryptographic technique in this context implies a particular cryptographic algorithm or process. Herz discloses changing cryptographic keys over time using a Vernam (one time pad) technique. Herz does not teach or suggest having a new cryptographic technique in the updated cryptographic software, because Herz uses the same technique all the time and just changes the key. This is not what is required by claim 24. Claim 24 has not been properly rejected. It is allowable as presented.

As to claim 25, Herz teaches nothing about tamper resistant software as that term is understood by those skilled in the art. Therefore, Herz teaches nothing about having the updated cryptographic software include a new tamper resistant technique.

As to claim 26, the cited text of Herz does not teach or suggest that the updated cryptographic software includes a new software configuration. Instead, Herz discloses that the **EPG data** on the set top box is updated, not the set top box **software**.

For independent claim 8, a similar rationale as stated above is applicable. Therefore, claim 8 is also allowable. Additionally, claim 11 is allowable since it is dependent from allowable claim 8.

As to independent claim 21, it contains similar limitations as allowable independent claim 1. Therefore, it is also allowable under the same rationale.

Claims 22-23 are also allowable for the same reasons as claims 6 and 7.

Claims 28-31 are dependent on allowable independent claim 21. Thus, they are also allowable.

CONCLUSION

In view of the foregoing, Claims 1, 4, 6-8, 11, and 21-31 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (503) 264-8074. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Date: December 28, 2006

/Steven P. Skabrat/
Steven P. Skabrat
Registration No. 36,279
Senior Attorney
Intel Corporation
(503) 264-8074

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026